Characters

Author: Jiahai Wang

Date: November 24, 2024

Contents

Chapter 1 Characters

1.1 Introduction

The characters on residue classes, both additive and multiplicative, play instrumental parts in analytic number theory. Other characters such as the Hecke characters of a number field, or the characters of a finite field are also indispensable in the modern theory. We shall introduce these in due course. However, to avoid redundancy we start here by giving basic definitions in a general context of a finite abelian group. (Characters for non-abelian groups occur also, but more naturally as Galois groups and are best seen from the automorphic perspective in analytic number theory).

Let G be a finite abelian group. A homomorphism $\chi : G \to \mathbb{C}^\star$ is called a character of G. Therefore (in the multiplicative notation) χ has the properties

$$\chi(xy) = \chi(x)\chi(y) \quad \text{for all } x, y \in G,$$

$\chi(1) = 1$ and $\chi(x)^m = 1$, where $m = |G|$ is the order of G, therefore $\chi(x)$ is a root of unity.
The characters of G form a group $\widehat{G}$ with multiplication given by

$$(\chi_1\chi_2)(x) = \chi_1(x)\chi_2(x) \quad \text{for all } x \in G.$$

$\widehat{G}$ **is called the dual group**, its identity element is the trivial character

$$\chi_0(x) = 1 \quad \text{for all } x \in G.$$

Throughout, $\bar{\chi}$ denotes the complex conjugate, hence also the inverse. If G is cyclic of order m and g is a generator of G, then every character of G is of type

$$\chi_a(x) = e^{2\pi i a y/m}, \quad \text{if } x = g^y$$

for some fixed residue class $a \pmod m$. These are distinct characters, therefore $\widehat{G}$ is also cyclic of order m, so $\widehat{G}$ is isomorphic to G. The isomorphism $\widehat{G} \simeq G$ can be established for any finite abelian group by writing G as the direct product of cyclic groups. There is a canonical isomorphism between G and $\widehat{\widehat{G}}$ given by $x \mapsto \widehat{\widehat{x}}$ where

$$\widehat{\widehat{x}}(\chi) = \chi(x) \quad \text{for all } \chi \in \widehat{G}.$$

The raison d'être of these characters is found in the following orthogonality relations

$$\sum_{x \in G} \chi(x) = \begin{cases} |G| & \text{if } \chi = \chi_0, \\ 0 & \text{if } \chi \neq \chi_0, \end{cases}$$

$$\sum_{\chi \in \widehat{G}} \chi(x) = \begin{cases} \left|\widehat{G}\right| & \text{if } x = 1, \\ 0 & \text{if } x \neq 1, \end{cases}$$

which allows us to detect the group identity element.

Suppose d divides the order of G. An element $g \in G$ is said to have exponent d if g^d is the identity. The order of g is its smallest exponent. The characters of exponent d are exactly those which are trivial on the subgroup

$$G^d = \left\{x^d : x \in G\right\}$$

therefore they may be viewed as characters of the factor group G/G^d. The orthogonality relations become

$$\sum_{\chi^d=\chi_0} \chi(y) = \begin{cases} [G:G^d] & \text{if } y \in G^d, \\ 0 & \text{if } y \notin G^d. \end{cases}$$

This will allow us to detect the d-th powers of G.

1.2 Dirichlet characters

First we consider the characters on the additive group $\mathbb{Z}/m\mathbb{Z}$ of residue classes modulo m . They are given by

$$\psi_a(n) = e\left(\frac{an}{m}\right)$$

where $e(z) = e^{2\pi iz}$. This formula makes an additive character a function on $\mathbb{Z}$, periodic of period m . The orthogonality property becomes

$$\sum_{a(\bmod m)} e\left(\frac{an}{m}\right) = \begin{cases} m & \text{if } n \equiv 0 (\bmod m), \\ 0 & \text{otherwise.} \end{cases}$$

We shall call $\psi_a(n) = e(an/m)$ primitive if $(a,m) = 1$. Adding all the additive primitive characters we obtain the Ramanujan sum

$$S(n,0;m) = c_m(n) = \sideset{}{^\star}\sum_{a(\bmod m)} e\left(\frac{an}{m}\right).$$

Recall that throughout this book $\sideset{}{^\star}\sum$ restricts the summation to "primitive" elements, in the above case among additive characters modulo m . One shows by Möbius inversion that

$$c_m(n) = \sum_{d|(m,n)} d\mu\left(\frac{m}{d}\right) \tag{1.1}$$

Hence

$$c_m(n) = \mu\left(\frac{m}{(m,n)}\right) \frac{\varphi(m)}{\varphi(m/(m,n))} \tag{1.2}$$

In particular,

$$c_m(n) = \mu(m) \text{ if } (m,n) = 1.$$

In general,

$$|c_m(n)| \leq (m,n)$$

Next we consider characters on the multiplicative group of residue classes $a (\bmod m)$ with $(a,m) = 1$,

$$\chi : (\mathbb{Z}/m\mathbb{Z})^\star \to \mathbb{C}$$

As with the additive characters, we wish to consider χ as a function on $\mathbb{Z}$; we do so by setting $\chi(n) = 0$ whenever n is not prime to m . This makes χ a Dirichlet character, a function on $\mathbb{Z}$, periodic modulo m and completely multiplicative. The corresponding extension of the trivial character $\chi_0 (\bmod m)$ is called the principal character to modulus m . The group $(\mathbb{Z}/m\mathbb{Z})^\star$ and its dual have $\varphi(m)$ elements. The orthogonality relations become

$$\sum_{a(\bmod m)} \chi(a) = \begin{cases} \varphi(m) & \text{if } \chi = \chi_0, \\ 0 & \text{otherwise,} \end{cases}$$

$$\sum_{\chi(\bmod m)} \chi(a) = \begin{cases} \varphi(m) & \text{if } a \equiv 1 \,(\bmod m), \\ 0 & \text{otherwise,} \end{cases}$$

If $m = m_1 m_2$ with $(m_1, m_2) = 1$, then $(\mathbb{Z}/m\mathbb{Z})^\star \simeq (\mathbb{Z}/m_1\mathbb{Z})^\star \times (\mathbb{Z}/m_2\mathbb{Z})^\star$, so every multiplicative character $\chi \,(\bmod m)$ is a product $\chi_1\chi_2$ of multiplicative characters $\chi_1 \,(\bmod m_1)$ and $\chi_2 \,(\bmod m_2)$. **The Dirichlet series associated to Dirichlet characters are of paramount importance in analytic number theory. They are called Dirichlet L-functions and denoted $L(s, \chi)$, or $L(\chi, s)$ depending on emphasis:**

$$L(s, \chi) = \sum_{n \geq 1} \chi(n) n^{-s} = \prod_p \left(1 - \chi(p) p^{-s}\right)^{-1};$$

the series and the Euler product are absolutely convergent for $\mathrm{Re}(s) > 1$. As is well known, these functions can be analytically continued to $\mathbb{C}$. See Section 4.6 for a proof. Many other analytic properties, applications and generalizations of Dirichlet L-functions will be considered throughout the book.

Note that by total multiplicativity,

$$\frac{1}{L(s, \chi)} = \sum_{n \geq 1} \mu(n) \chi(n) n^{-s}, \; -\frac{L'}{L}(s, \chi) = \sum_{n \geq 1} \Lambda(n) \chi(n) n^{-s}$$

for $\mathrm{Re}(s) > 1$.

1.3 Primitive characters

Associated to each character χ, in addition to its modulus m, is a natural number $m^\star$, its conductor. The conductor is the smallest divisor of m such that χ may be written as $\chi = \chi_0 \chi^\star$ where χ_0 is the principal character to modulus m and $\chi^\star$ is a character to modulus $m^\star$. For some characters the conductor is equal to the modulus. Such characters are called primitive. In the above factorization $\chi^\star$ is a primitive character uniquely determined by χ. **We shall say that χ is induced by $\chi^\star$ or that $\chi^\star$ induces χ. We have**

$$\chi(a) = \chi^\star(a) \;\text{ if }\; (a, m) = 1.$$

The number of primitive characters to modulus m is given by

$$\varphi^\star(m) = m \prod_{p \| m} \left(1 - \frac{2}{p}\right) \prod_{p^2 | m} \left(1 - \frac{1}{p}\right)^2 \tag{1.3}$$

The proof is a simple exercise in Möbius inversion. Indeed, we have $\varphi = 1 \star \varphi^\star$, whence $\varphi^\star = \mu \star \varphi$, i.e.,

$$\varphi^\star(m) = \sum_{d | m} \mu(d) \varphi\left(\frac{m}{d}\right)$$

giving 1.3 by multiplicativity. In the same way using the orthogonality of characters we infer a more general result

$$\sideset{}{^\star}\sum_{\chi(\bmod m)} \chi(a) = \sum_{d | (a-1, m)} \varphi(d) \mu\left(\frac{m}{d}\right) \;\text{ if }\; (a, m) = 1.$$

Incidentally, the formula 1.3 shows that the primitive characters $\chi \,(\bmod m)$ exist precisely when $m 2 \,(\bmod 4)$.

The primitive characters are pleasant to deal with. For example, we have a convenient formula (which is not valid for χ not primitive)

(3.9)

$$\frac{1}{m}\sum_{c(\bmod m)}\chi(ac+b)=\begin{cases}\chi(b) & \text{if } m\mid a\\ 0 & \text{if } m\nmid a\end{cases}$$

Indeed, letting S be the above sum we obtain $\chi(1+m_1x)S=S$ for any x, where $m_1=m(a,m)/(a^2,m)$. If $S\neq 0$, this yields $\chi(1+m_1x)=1$ for any x, which implies that χ is periodic of period m_1. Since χ is primitive, we must have $m_1=m$, i.e., $m\mid a$. Thus $S=0$ if $m\nmid a$, and (3.9) is obvious otherwise.

The Dirichlet characters of exponent two are just the real characters (real-valued). In a number of ways they play a special role, particularly they are fundamental in the theory of quadratic forms. Below we give a complete list of real primitive characters. If $m=p$ is an odd prime, then there exists exactly one real primitive character of conductor p, **namely the quadratic residue symbol (the Legendre symbol)**

$$\chi_p(n)=\left(\frac{n}{p}\right)$$

This can be defined by saying that $1+\chi_p(n)$ is the number of solutions $x(\bmod p)$ to $x^2\equiv n(\bmod p)$.

For $m=4$ we have exactly one primitive character defined by

$$\chi_4(n)=(-1)^{\frac{n-1}{2}}\quad\text{if } 2\nmid n.$$

If $m=8$, we have two primitive characters

$$\chi_8(n)=(-1)^{\frac{1}{8}(n-1)(n+1)}\text{ if } 2\nmid n,$$

$$\chi_4\chi_8(n)=(-1)^{\frac{1}{8}(n-1)(n+5)}\quad\text{if } 2\nmid n.$$

If m is prime power, there are no real primitive characters of conductor m other than $\chi_4,\chi_8,\chi_4\chi_8$ and χ_p. Every real primitive character $\chi(\bmod m)$ is obtained as the product of the above ones. Therefore the conductor of a real primitive character is a number of type $1,k,4k,8k$ where k is a positive odd and squarefree integer.

1.4 Gauss sums

Let us come back for a moment to a general finite abelian group G. The characters of G form a complete orthogonal system so that any function $f:G\to\mathbb{C}$ has the Fourier expansion

$$f=\frac{1}{|G|}\sum_{\psi\in\widehat{G}}\langle f,\psi\rangle\psi$$

with coefficients

$$\langle f,\psi\rangle=\sum_{g\in G}f(g)\bar{\psi}(g)$$

✍ **Exercise 1.1DUE TO DEDEKIND** Prove that

$$\prod_{\psi\in\widehat{G}}\langle f,\psi\rangle=\det_{g,h\in G}\left(f\left(gh^{-1}\right)\right)$$

In the case of functions on residue classes, and on a finite field, both additive and multiplicative characters are present and it is often necessary to transform the Fourier expansion in one of these systems to the other. In doing so we encounter Gauss sums $\langle\chi,\psi\rangle$ for any pair of multiplicative and additive characters χ,ψ respectively. We shall present the Gauss sums for finite fields in due time.

Now we consider Gauss sums associated with characters on residue classes, say modulo m. For any multiplicative character $\chi(\bmod m)$ we put

$$\tau(\chi) = \sum_{b(\bmod m)} \chi(b)\, e\left(\frac{b}{m}\right).$$

Multiplying by $\bar{\chi}(a)$ and summing over χ we derive by orthogonality

$$e\left(\frac{a}{m}\right) = \frac{1}{\varphi(m)} \sum_{\chi(\bmod m)} \bar{\chi}(a)\,\tau(\chi) \quad \text{if } (a,m)=1.$$

This is the Fourier expansion of additive characters in terms of the multiplicative ones. Similarly

$$\chi(a)\,\tau(\bar{\chi}) = \sum_{b(\bmod m)} \bar{\chi}(b)\, e\left(\frac{ab}{m}\right) \quad \text{if } (a,m)=1$$

which gives the Fourier expansion of χ in terms of additive characters provided $\tau(\bar{\chi}) \neq 0$. Note that the condition $(a,m)=1$ in (3.12) can be dropped if χ is primitive because both sides vanish if $(a,m) \neq 1$.

Lemma 1.1

Suppose the character χ modulo m is induced by the primitive character $\chi^\star$ modulo $m^\star$. Then

$$\tau(\chi) = \mu\left(\frac{m}{m^\star}\right)\chi^\star\left(\frac{m}{m^\star}\right)\tau(\chi^\star).$$

If $\chi(\bmod m)$ is primitive, then

$$|\tau(\chi)| = \sqrt{m}$$

♡

Proof We have

$$\tau(\chi) = \sum_{a(\bmod m)}^{\star} \chi^\star(a)\, e\left(\frac{a}{m}\right) = \sum_{d|m} \mu(d)\,\chi^\star(d) \sum_{a(\bmod \frac{m}{d})} \chi^\star(a)\, e\left(\frac{ad}{m}\right).$$

The innermost sum vanishes unless $d = m/m^\star$ giving (3.13). To prove (3.14) we write

$$|\tau(\chi)|^2 = \sum_{a,b(\bmod m)} \sum_{\chi(a)} \chi(a)\,\bar{\chi}(b)\, e\left(\frac{a-b}{m}\right)$$

$$= \sum_{a(\bmod m)} \chi(a) \sum_{b(\bmod m)}^{\star} e\left(\frac{(a-1)\,b}{m}\right).$$

The inner sum is the Ramanujan sum (which is also the Gauss sum for the principal character).we get

$$|\tau(\chi)|^2 = \sum_{d|m} d\mu\left(\frac{m}{d}\right) \sum_{\substack{a(\bmod m) \\ a\equiv 1(\bmod d)}} \chi(a).$$

If χ is primitive of conductor m, then the last sum vanishes unless $d = m$

One can see by Lemma 1.1 that $\tau(\chi)$ does not vanish exactly when $m/m^\star$ is squarefree and prime to $m^\star$.

We now consider the more general sum

$$\tau(\chi, \psi_a) = \sum_{b(\bmod m)} \chi(b)\,\psi_a(b)$$

where $\psi_a(b) = e(ab/m)$ is an additive character.

Lemma 1.2

Let χ modulo m be a non-principal character induced by the primitive character $\chi^\star$ modulo $m^\star$. Let $a \geq 1$. We have

$$\tau(\chi, \psi_a) = \tau(\chi) \sum_{d|(a,m/m^\star)} d\bar{\chi}^\star(a/d)\,\mu(m/dm^\star), \tag{1.4}$$

in particular,

$$\tau(\chi, \psi_a) = \bar{\chi}(a)\,\tau(\chi)$$

if $(a, m) = 1$, i.e. if ψ_a is a primitive additive character.

♡

Note that $\bar{\tau}(\chi) = \chi(-1)\,\tau(\bar{\chi})$, hence if $\chi \pmod m$ is primitive, then (1.4) can be written as

$$\tau(\chi)\,\tau(\bar{\chi}) = \chi(-1)\,m$$

For any characters $\chi_1 \pmod{m_1}$ and $\chi_2 \pmod{m_2}$ with $(m_1, m_2) = 1$ we have

$$\tau(\chi_1\chi_2) = \chi_1(m_2)\,\chi_2(m_1)\,\tau(\chi_1)\,\tau(\chi_2)$$

This multiplication rule fails if the moduli are not relatively prime. For characters to the same modulus the correction factor is the Jacobi sum

$$J(\chi_1, \chi_2) = \sum_{a \pmod m} \chi_1(a)\,\chi_2(1-a).$$

Precisely if χ_1, χ_2 are two characters modulo m such that $\chi_1\chi_2$ is primitive, then

$$\tau(\chi_1)\,\tau(\chi_2) = J(\chi_1, \chi_2)\,\tau(\chi_1\chi_2)$$

Hence if all $\chi_1, \chi_2, \chi_1\chi_2$ are primitive of modulus m, then

$$|J(\chi_1, \chi_2)| = \sqrt{m}$$

If $\chi \pmod m$ is primitive, then

$$J(\chi, \bar{\chi}) = \chi(-1)\,\mu(m)$$

1.5 Real characters

For a primitive character $\chi \pmod m$ we know that $|\tau(\chi)| = \sqrt{m}$, however, the determination of the argument of $\tau(\chi)$ is a difficult problem. Using Deligne's estimate for multiple Kloosterman sums one can show that $\tau(\chi)/\sqrt{m}$ are asymptotically equidistributed on the unit circle as $\chi \pmod m$ ranges over all primitive characters and m tends to infinity over primes.

In the case of real characters $\tau(\chi)$ were evaluated completely by Gauss. It is easy to see that $\tau(\chi_4) = 2i, \tau(\chi_8) = 2\sqrt{2}$ and $\tau(\chi_4\chi_8) = 2\sqrt{2}i$.

Theorem 1.1

(GAUSS). For m odd squarefree

$$\tau(\chi) = \varepsilon_m\sqrt{m}$$

where

$$\varepsilon_m = \begin{cases} 1 & \text{if } m \equiv 1 \pmod 4 \\ i & \text{if } m \equiv -1 \pmod 4 \end{cases}$$

♡

We shall give an analytic proof . But first we evaluate other Gauss sums of type

$$G(m) = \sum_{n \pmod m} e\left(\frac{n^2}{m}\right)$$

for any integer $m \geq 1$. If m is even we derive by shifting n to $n+\frac{m}{2}$ that $G(m) = i^m G(m)$, because $\frac{1}{m}\left(n+\frac{m}{2}\right)^2 \equiv \frac{n^2}{m} + \frac{m}{4} \pmod 1$. Hence

$$G(m) = 0, \quad \text{if } m \equiv 2 \pmod 4 .$$

Next we show that

$$G\left(m^3\right) = mG(m), \quad \text{if } m2 \pmod 4 .$$

This follows by splitting the summation in $G\left(m^3\right)$ into $n \equiv a+bm^2 \pmod{m^3}$ if $2 \nmid m$ or $n \equiv a+b\frac{m^2}{2} \pmod{m^3}$ if $4 \mid m$. Now we are ready to prove

Theorem 1.2 (DIRICHLET)

For any $m \in \mathbb{N}$,

$$\bar{G}(m) = \frac{1+i^m}{1+i}\sqrt{m}$$

♡

Proof We have

$$G(m) = 2\sum_{0<n<\frac{m}{2}} e\left(\frac{n^2}{m}\right) + O(1)$$

In the segment $\frac{m}{4} < n < \frac{m}{2}$ we change n into $\left[\frac{m}{2}\right] - n = \frac{m}{2} - \left\{\frac{m}{2}\right\} - n$. Since

$$\begin{aligned} \frac{1}{m}\left(\left[\frac{m}{2}\right]-n\right)^2 &= \frac{1}{m}\left(n+\left\{\frac{m}{2}\right\}\right)^2 - \frac{m}{4} + \left[\frac{m}{2}\right] - n \\ &\equiv \frac{1}{m}\left(n+\left\{\frac{m}{2}\right\}\right)^2 - \frac{m}{4} \pmod 1 \end{aligned}$$

we obtain

$$G(m) = 2\sum_{0<n<\frac{m}{4}} e\left(\frac{n^2}{m}\right) + 2i^{-m}\sum_{0<n<\frac{m}{4}} e\left(\frac{(n+\{m/2\})^2}{m}\right) + O(1) .$$

Here, and as before, the error term $O(1)$ accounts for the terms which are not covered in the displayed summation (at most two of them).

$$\int_0^{m/4} e\left(\frac{x^2}{m}\right) dx = \int_0^{\infty} e\left(\frac{x^2}{m}\right) dx + O(1) = \frac{1+i}{4}\sqrt{m} + O(1) .$$

Hence adding up these results we get

$$G(m) = \frac{1+i^{-m}}{1+i^{-1}}\sqrt{m} + O(1) .$$

It remains to show that the last error term $O(1)$ vanishes.

We generalize $G(m)$ by setting

$$G\left(\frac{a}{m}\right)=\sum_{n(\bmod m)}e\left(\frac{an^2}{m}\right)$$

for any a with $(a,m)=1$. In particular, $G\left(\frac{1}{m}\right)=G(m)$. If $m=m_1m_2$ with $(m_1,m_2)=1$, we obtain

$$G\left(\frac{a}{m_1m_2}\right)=G\left(\frac{am_2}{m_1}\right)G\left(\frac{am_1}{m_2}\right)$$

by writing $n=n_1m_2+n_2m_1$ with n_1 and n_2 ranging modulo m_1 and m_2 respectively. This formula reduces the problem of evaluating generalized Gauss sum $G(a/m)$ to that of a prime power modulus. If $m=p$ is an odd prime we can write

$$G\left(\frac{a}{p}\right)=\sum_{b(\bmod p)}\left(1+\left(\frac{b}{p}\right)\right)e\left(\frac{ab}{p}\right)$$

since $1+\left(\frac{b}{p}\right)$ is the number of solutions to $n^2\equiv b\,(\bmod p)$. Therefore

$$G\left(\frac{a}{p}\right)=\sum_{b(\bmod p)}\left(\frac{b}{p}\right)e\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)G\left(\frac{1}{p}\right)=\left(\frac{a}{p}\right)\varepsilon_p\sqrt{p}$$

$$\varepsilon_{pq}\sqrt{pq}=G\left(\frac{1}{pq}\right)=G\left(\frac{p}{q}\right)G\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)\varepsilon_p\varepsilon_q\sqrt{pq}. \tag{1.5}$$

Note also that

$$\varepsilon_{pq}=\varepsilon_p\varepsilon_q(-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{1.6}$$

Combining these formulas we deduce

Theorem 1.3 (QUADRATIC RECIPROCITY LAW)

For any odd primes $p\neq q$ we have

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{1.7}$$

Since $G(-1/p)=\bar{G}(1/p)$ it follows from (3.29) that for odd p

$$\left(\frac{-1}{p}\right)=\varepsilon_p^2=(-1)^{\frac{p-1}{2}}=\chi_4(p).$$

♡

✍ **Exercise 1.2** Prove that for odd p ,

$$\left(\frac{2}{p}\right)=(-1)^{\frac{1}{8}\left(p^2-1\right)}=\chi_8(p)$$

Note we have proved that

$$\sum_{x(\bmod m)}\left(\frac{x}{m}\right)e\left(\frac{x}{m}\right)=\sum_{x(\bmod m)}e\left(\frac{x^2}{m}\right)$$

if m is odd squarefree. If m is odd but not squarefree, the left side vanishes while the right side does not. For convenience we extend the Legendre symbol $\left(\frac{a}{p}\right)$ to $p=2$ by setting

$$\left(\frac{a}{2}\right)=\begin{cases}1 & \text{if } 2\nmid a\\ 0 & \text{if } 2\mid a\end{cases}$$

Then for any $b>0$ we define

$$\left(\frac{a}{b}\right) = \prod_{p^v \| b} \left(\frac{a}{p}\right)^{\nu}$$

If b is odd, this symbol $\left(\frac{a}{b}\right)$ was introduced by Jacobi.

✍ **Exercise 1.3** for any odd integers a, b relatively prime

$$\left(\frac{a}{|b|}\right)\left(\frac{b}{|a|}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}(a,b)_\infty.$$

Here $(x,y)_\infty$ is the Hilbert symbol defined for $xy \neq 0$ by

$$(x,y)_\infty = \begin{cases} -1 & \text{if } x<0 \text{ and } y<0 \\ 1 & \text{otherwise.} \end{cases}$$

Notice that $2(x,y)_\infty = 1 + \operatorname{sign} x + \operatorname{sign} y - \operatorname{sign} xy$.

✍ **Exercise 1.4** Prove that for any a, m with $(2a, m) = 1$,

$$G\left(\frac{a}{m}\right) = \left(\frac{a}{m}\right)\varepsilon_m\sqrt{m}$$

Finally we extend the symbol $\left(\frac{a}{b}\right)$ to all integers a, b except for $a = b = 0$. If $ab \neq 0$, we set

$$\left(\frac{a}{b}\right) = \left(\frac{a}{|b|}\right)(a,b)_\infty$$

Then we set

$$\left(\frac{1}{0}\right) = \left(\frac{0}{1}\right) = \left(\frac{0}{-1}\right) = -\left(\frac{-1}{0}\right) = 1$$

and

$$\left(\frac{a}{b}\right) = 0 \text{ if } (a,b) \neq 1$$

✍ **Exercise 1.5** Check the consistency of the above settings. Prove that for any $b \geq 1$ the map $a \mapsto \left(\frac{a}{b}\right)$ is a Dirichlet character modulo b. Prove that for any $a \neq 0$ the map $b \mapsto \left(\frac{a}{b}\right)$ is a Dirichlet character of conductor $a^\star \mid 4a$.

The above extension of $\left(\frac{a}{b}\right)$ will be called the **Jacobi symbol**

Any integer $\Delta \neq 0$ with $\Delta \equiv 0, 1 \pmod 4$ is called a discriminant. If $\Delta = 1$ or Δ is the discriminant of a quadratic field, then Δ is said to be fundamental. Any discriminant can be written uniquely as $\Delta = e^2 D$ with D fundamental and $e \geq 1$. A prime discriminant is a fundamental discriminant having exactly one prime factor, thus it is a number of type $-4, -8, 8$ and $\chi_4(p)\, p$ with $p > 2$. Every fundamental discriminant factors into prime discriminants.

To any discriminant Δ one associates **the Kronecker symbol** $\left(\frac{\Delta}{c}\right)_K$ which is defined for any $c \neq 0$ by means of the Jacobi symbol as follows

$$\left(\frac{\Delta}{c}\right)_K = \left(\frac{2^\nu}{\Delta}\right)\left(\frac{\Delta}{b}\right) \tag{1.8}$$

where $c = 2^\nu b$ with b odd. Note that $\left(\frac{\Delta}{2}\right)_K = \left(\frac{2}{\Delta}\right) = \chi_8(\Delta)$, explicitly

$$\left(\frac{\Delta}{2}\right)_K = \begin{cases} 1 & \text{if } \Delta \equiv 1 \pmod 8 \\ -1 & \text{if } \Delta \equiv 5 \pmod 8 \\ 0 & \text{if } \Delta \equiv 0 \pmod 4 \end{cases} \tag{1.9}$$

We also extend the definition of the Kronecker symbol for $c = 0$ by setting

$$\left(\frac{\Delta}{0}\right)_K = \begin{cases} 1 & \text{if } \Delta = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Therefore $\left(\frac{\Delta}{c}\right)_K$ is defined for all integers c and $\Delta \neq 0, \Delta \equiv 0, 1 \pmod 4$.

We shall drop the subscript K in the Kronecker symbol notation and explain in any relevant case that we are dealing with the Kronecker symbol. Remember the Kronecker symbol is not defined for Δ 's other than discriminants. When the symbol $\left(\frac{\Delta}{c}\right)$ appears without comments it stands for the Jacobi symbol.

✍ **Exercise 1.6** Prove that for a fundamental discriminant Δ the Kronecker symbol $\left(\frac{\Delta}{c}\right)$ is a primitive character of conductor $|\Delta|$.

1.6 The quartic residue symbol

Next we construct certain characters of order four. These are associated with $\mathbb{Q}(i)$, the imaginary quadratic field of discriminant $D = -4$. The ring of integers of $\mathbb{Q}(i)$ is

$$\mathbb{Z}[i] = \{z = a + bi : a, b \in \mathbb{Z}\}$$

and the group of units of $\mathbb{Z}[i]$ is $\{1, i, i^2, i^3\}$. The irreducible elements of $\mathbb{Z}[i]$ are (up to the units); $1 + i$ with $N(1 + i) = 2$, the rational primes $q \equiv -1 \pmod 4$ with $Nq = q^2$ and the complex numbers $\pi = a + bi$ with

$$N\pi = \pi\bar{\pi} = a^2 + b^2 = p \equiv 1 \pmod 4.$$

Note that π and $\bar{\pi}$ are coprime, these are called Gaussian primes. Every element of $\mathbb{Z}[i]$ different from zero factors uniquely (up to the units and permutations) into powers of irreducible elements.

For every Gaussian prime π we define a map (the quartic residue symbol)

$$\left(\frac{\alpha}{\pi}\right) : \mathbb{Z}[i] \to \{0, 1, i, i^2 i^3\}$$

which satisfies

$$\left(\frac{\alpha}{\pi}\right) \equiv \alpha^{\frac{p-1}{4}} \pmod \pi$$

Note that $\left(\frac{\alpha}{\pi}\right) = 0$ if $\pi \mid \alpha$. If $\pi \nmid \alpha$, then $\alpha^{p-1} \equiv 1 \pmod \pi$ because the residue class ring $\mathbb{Z}\left[i\right]/\pi\mathbb{Z}[i]$ is a finite field with $p = N\pi$ elements. This property (the little theorem of Fermat) implies the existence and the uniqueness of solutions with $\left(\frac{\alpha}{\pi}\right) = i^m$ for some $0 \leq m < 4$. In particular, we have

$$\left(\frac{i}{\pi}\right) = i^{\frac{p-1}{4}}, \quad \text{if } p = \pi\bar{\pi} \equiv 1 \pmod 4.$$

✍ **Exercise 1.7** Prove the following properties of the quartic residue symbol:

$$\left(\frac{\alpha\beta}{\pi}\right) = \left(\frac{\alpha}{\pi}\right)\left(\frac{\beta}{\pi}\right)$$

$$\alpha \equiv \beta \pmod \pi \Rightarrow \left(\frac{\alpha}{\pi}\right) = \left(\frac{\beta}{\pi}\right)$$

$$\left(\frac{\alpha}{\pi'}\right) = \left(\frac{\alpha}{\pi}\right) \quad \text{if } \pi' = \pi i^m$$

$$\left(\frac{\bar{\alpha}}{\bar{\pi}}\right) = \left(\frac{\bar{\alpha}}{\pi}\right)$$

$$\left(\frac{\alpha}{\pi}\right)=1$$

if and only if

$$z^4\equiv\alpha\,(\bmod\ \pi)$$

has a solution in

$$\mathbb{Z}[i]^\star$$

.

If $\gamma=\pi_1\cdots\pi_r$ is the product of Gaussian primes (not necessarily distinct), then we set the symbol

$$\left(\frac{\alpha}{\gamma}\right)=\left(\frac{\alpha}{\pi_1}\right)\cdots\left(\frac{\alpha}{\pi_r}\right)$$

Clearly the properties hold true with π replaced by γ . In particular,

$$\left(\frac{\alpha}{p}\right)=1\ \text{ if }\ (\alpha,p)=1$$

Note that $(1+i)^2=2i$. We say that $\alpha\in\mathbb{Z}[i]$ is odd if $(1+i)\nmid\alpha$ and primary if $\alpha\equiv1\,(\bmod\ 2(1+i))$. Every odd number in $\mathbb{Z}[i]$ is associated with exactly one primary element, i.e., $\varepsilon\alpha\equiv1\,(\bmod\ 2(1+i))$ for exactly one unit $\varepsilon=i^m$. A primary element can be written as the product of primary irreducibles uniquely up to permutations. We have the following

Theorem 1.4 (THE LAW OF QUARTIC RECIPROCITY)

If π_1,π_2 are distinct primary Gaussian primes, then

$$\left(\frac{\pi_1}{\pi_2}\right)\left(\frac{\pi_2}{\pi_1}\right)=(-1)^{\frac{p_1-1}{4}\frac{p_2-1}{4}}$$

where $p_1=N\pi_1$ and $p_2=N\pi_2$. If $\pi=a+bi$ is primary, then

$$\left(\frac{i}{\pi}\right)=i^{(1-a)/2},\ \left(\frac{1+i}{\pi}\right)=i^{\left(a-1-b-b^2\right)/4},\ \left(\frac{2}{\pi}\right)=i^{-b/2}.$$

♡

The quartic residue symbol $\left(\frac{\alpha}{\pi}\right)$ is a multiplicative character of the finite field $\mathbb{F}_p\simeq\mathbb{Z}[i]/\pi\mathbb{Z}[i]$. The Gauss sum of this character is

$$g(\pi)=\sum_{a(\bmod\ p)}\left(\frac{\alpha}{\pi}\right)e\left(\frac{a}{p}\right)$$

where a runs over the rational residue classes modulo p and α is the representative of a in $\mathbb{Z}[i]$ modulo π . If π is primary, then

$$g^2(\pi)=-(-1)^{\frac{p-1}{4}}\pi\sqrt{p}$$

We shall be interested in the quartic residue symbol at rational integers

$$\chi_\pi(n)=\left(\frac{n}{\pi}\right),\ \text{ for } n\in\mathbb{Z}.$$

This is a Dirichlet character of conductor $p=\pi\bar{\pi}$ and of order four. Since $(\pi,\bar{\pi})=1$, we have $\chi_\pi^2(n)\equiv n^{\frac{p-1}{2}}\,(\bmod\ p)$. Therefore

$$\chi_\pi^2(n)=\left(\frac{n}{p}\right)$$

is the quadratic residue symbol. Clearly $\chi_\pi(n)$ and $\chi_{\bar\pi}(n)$ are distinct Dirichlet characters but their squares yield the same quadratic character. More generally, if $q = p_1 \cdots p_r$ is the product of distinct primes $p_j \equiv 1 \pmod 4$, then there are 2^r distinct Dirichlet characters $\chi \pmod q$ satisfying $\chi^2 = \chi_q$, namely $\chi = \chi_{\pi_1} \cdots \chi_{\pi_r} = \chi_\gamma$, say, for any $\gamma = \pi_1 \cdots \pi_r$ with $\gamma\bar\gamma = q$.

1.7 The Jacobi-Dirichlet and the Jacobi-Kubota symbols

Let q be the product of primes $\equiv 1 \pmod 4$ (not necessarily distinct primes). The Jacobi symbol $\chi_q(n) = \left(\frac{n}{q}\right)$ can be extended to Gaussian domain $\mathbb{Z}[i]$ in several ways corresponding to representations of q as the sum of two squares

$$q = u^2 + v^2 \text{ with } (u, v) = 1.$$

By requiring $w = u + iv$ to be primary we distinguish u from v and we fix the sign of u. Note that $u \equiv 1 \pmod 2$ and $v \equiv u - 1 \pmod 4$. A Gaussian integer $w = u + iv$ is said to be primitive if $(u, v) = 1$, thus an odd w is primitive if $(w, \bar w) = 1$. For any primary primitive w we define the symbol $\left(\frac{z}{w}\right) : \mathbb{Z}[i] \to \{0, 1, -1\}$ by

$$\left(\frac{z}{w}\right) = \left(\frac{\operatorname{Re} wz}{|w|^2}\right)$$

where on the right side is the Jacobi symbol. More explicitly we have

$$\left(\frac{z}{w}\right) = \left(\frac{ur - vs}{q}\right), \quad \text{if } z = r + is$$

where $q = w\bar w$. If q is prime $\equiv 1 \pmod 4$, **we get two different symbols $\left(\frac{z}{w}\right)$ and $\left(\frac{z}{w}\right)$ which were considered by Dirichlet [Dir]. Throughout we call $\left(\frac{z}{w}\right)$ the Jacobi-Dirichlet symbol whenever w is primary and primitive.**

We could introduce the Jacobi-Dirichlet symbols using roots of quadratic congruences: there is one-to-one correspondence between the roots of

$$\omega^2 + 1 \equiv 0 \pmod q$$

and the factorizations $q = w\bar w$ with $w = u + iv$ primary which is given by

$$\omega \equiv -\bar u v \pmod q$$

Here $\bar u$ denotes the multiplicative inverse of u modulo q. We obtain

$$\left(\frac{z}{w}\right) = \left(\frac{r + \omega s}{q}\right) \quad \text{if } z = r + is$$

by $\left(\frac{u}{q}\right) = \left(\frac{|u|}{q}\right) = \left(\frac{q}{|u|}\right) = \left(\frac{v^2}{|u|}\right) = 1$. Hence it is clear that

$$\left(\frac{r}{w}\right) = \left(\frac{r}{q}\right) \quad \text{if } r \in \mathbb{Z}$$

For $z = i$ we have

$$\left(\frac{i}{w}\right) = i^{\frac{p-1}{2}}$$

Clearly $\left(\frac{z}{w}\right)$ is periodic in z of period q, and it is multiplicative as well since

$$(r_1 + \omega s_1)(r_2 + \omega s_2) \equiv r_1 r_2 - s_1 s_2 + \omega(r_1 s_2 + r_2 s_1) \pmod q.$$

✍ **Exercise 1.8** Derive from the quadratic reciprocity law the following reciprocity law for the Jacobi-Dirichlet symbol

$$\left(\frac{z}{w}\right) = \left(\frac{w}{z}\right)$$

for any z and w which are primary and primitive.

For Gaussian integers $z = r + is \equiv 1 \pmod 2$, we define

$$[z] = i^{\frac{r-1}{2}} \left(\frac{s}{|r|}\right)$$

where $\left(\frac{s}{|r|}\right)$ stands for the Jacobi symbol. Note that $[z]$ vanishes if z is not primitive. We are interested in the multiplicative structure of $[z]$ within the Gaussian ring $\mathbb{Z}[i]$ rather than with respect to the co-ordinates $(r, s) \in \mathbb{Z} \times \mathbb{Z}$. For this reason we refer to $[z]$ as the Jacobi-Kubota symbol. Indeed, this symbol is relevant to the Kubota homomorphism $SL(2, \mathbb{Z}) \to \{\pm 1\}$ which has much to do with metaplectic modular forms. Of course, $[z]$ is not multiplicative in the strict sense, yet it is nearly so, up to a factor which is the Jacobi-Dirichlet symbol.

✍ **Exercise 1.9** Prove that if w is primary primitive and $z \equiv 1 \pmod 2$, then

$$[wz] = \varepsilon [w] [z] \left(\frac{z}{w}\right)$$

with $\varepsilon = \pm 1$ depending only on the quadrants to which z, w and wz belong

Both symbols of Jacobi-Dirichlet and Jacobi-Kubota are utilized in the proof of the asymptotic formula for primes $p = X^2 + Y^4$. They play a role through the estimation for general bilinear forms in $[wz]$

Bibliography

[1] Analytic Number Theory Henryk Iwaniec: Rutgers University, Piscataway, NJ Emmanuel Kowalski : Université Bordeaux I, Talence, France

[2] Introduction to Analytic Number Theory Tom M. Apostol